

Requested Patent: EP0449242A2

Title:

METHOD AND STRUCTURE FOR PROVIDING COMPUTER SECURITY AND  
VIRUS PREVENTION. ;

Abstracted Patent: EP0449242 ;

Publication Date: 1991-10-02 ;

Inventor(s): LEE R JEFF (US); WATSON BRUCE WILLIAM (US) ;

Applicant(s): NAT SEMICONDUCTOR CORP (US) ;

Application Number: EP19910104834 19910327 ;

Priority Number(s): US19900500755 19900328 ;

IPC Classification: G06F11/00 ;

Equivalents: ;

#### ABSTRACT:

Tests are performed prior to or during the boot operation to determine whether files are corrupted. This may indicate the presence of a virus. If a potential error is detected, boot is halted, allowing the user to boot from uncorrupted files. In another embodiment, an uniquely formatted floppy diskette is used as an access diskette serves as a hardware key to gain access. In another embodiment, a host controls information stored locally. In another embodiment, security from unauthorized access is provided once a valid user has legitimately accessed a computer. In response to a predefined hot key or a predetermined period of time during which the user has not provided input, portions of the computer are disabled. Upon entry of access information by the valid user, the disabled features are enabled. In another embodiment, access to the computer is made more difficult in response to invalid access attempts. In one embodiment, once a threshold number of invalid access attempts is reached, the computer is locked up, requiring reboot, thereby increasing the difficulty of a would be intruder to gain access to the computer. In one embodiment, once the threshold value is reached, it is reset to a lower value.



⑫

## EUROPEAN PATENT APPLICATION

⑬ Application number: 91104834.6

⑮ Int. Cl.5: G06F 11/00

⑯ Date of filing: 27.03.91

⑭ Priority: 28.03.90 US 500755

⑮ Date of publication of application:  
02.10.91 Bulletin 91/40

⑯ Designated Contracting States:  
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

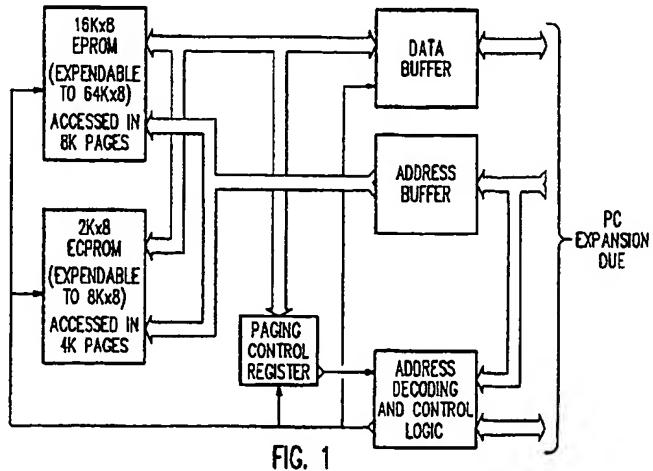
⑰ Applicant: NATIONAL SEMICONDUCTOR  
CORPORATION  
2900 Semiconductor Drive P.O. Box 58090  
Santa Clara California 95051-8090(US)

⑰ Inventor: Watson, Bruce William  
5615 Fort Fisher Way  
Norcross, Georgia 30092(US)  
Inventor: Lee, R. Jeff  
2581 Deer Isle Cove  
Lawrenceville, Georgia 30244(US)

⑰ Representative: Sparing Röhl Henseler  
Patentanwälte European Patent Attorneys  
Rethelstrasse 123  
W-4000 Düsseldorf 1(DE)

⑯ Method and structure for providing computer security and virus prevention.

⑰ Tests are performed prior to or during the boot operation to determine whether files are corrupted. This may indicate the presence of a virus. If a potential error is detected, boot is halted, allowing the user to boot from uncorrupted files. In another embodiment, an uniquely formatted floppy diskette is used as an access diskette serves as a hardware key to gain access. In another embodiment, a host controls information stored locally. In another embodiment, security from unauthorized access is provided once a valid user has legitimately accessed a computer. In response to a predefined hot key or a predetermined period of time during which the user has not provided input, portions of the computer are disabled. Upon entry of access information by the valid user, the disabled features are enabled. In another embodiment, access to the computer is made more difficult in response to invalid access attempts. In one embodiment, once a threshold number of invalid access attempts is reached, the computer is locked up, requiring reboot, thereby increasing the difficulty of a would be intruder to gain access to the computer. In one embodiment, once the threshold value is reached, it is reset to a lower value.



This invention pertains to electronic computers, and more specifically to security systems for use with electronic systems. The teachings of this invention are particularly useful for providing security in computer networks having more than one computer, for example a computer network including a plurality of PCs and a larger computer, such as a mainframe, serving as a host.

5 The overall computer security strategy of a computer network is only as strong as its weakest link, and unsecured PCs connected to mainframes represent an extremely weak link. For instance, authorized PC users can legitimately download large amounts of mainframe information. This data, which had been protected by the mainframe's access control facilities, is then easily accessed by anyone who can turn on the PC. Unauthorized users can copy sensitive data, modify data that will be uploaded to the mainframe, or  
 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95 100 105 110 115 120 125 130 135 140 145 150 155 160 165 170 175 180 185 190 195 200 205 210 215 220 225 230 235 240 245 250 255 260 265 270 275 280 285 290 295 300 305 310 315 320 325 330 335 340 345 350 355 360 365 370 375 380 385 390 395 400 405 410 415 420 425 430 435 440 445 450 455 460 465 470 475 480 485 490 495 500 505 510 515 520 525 530 535 540 545 550 555 560 565 570 575 580 585 590 595 600 605 610 615 620 625 630 635 640 645 650 655 660 665 670 675 680 685 690 695 700 705 710 715 720 725 730 735 740 745 750 755 760 765 770 775 780 785 790 795 800 805 810 815 820 825 830 835 840 845 850 855 860 865 870 875 880 885 890 895 900 905 910 915 920 925 930 935 940 945 950 955 960 965 970 975 980 985 990 995 1000 1005 1010 1015 1020 1025 1030 1035 1040 1045 1050 1055 1060 1065 1070 1075 1080 1085 1090 1095 1100 1105 1110 1115 1120 1125 1130 1135 1140 1145 1150 1155 1160 1165 1170 1175 1180 1185 1190 1195 1200 1205 1210 1215 1220 1225 1230 1235 1240 1245 1250 1255 1260 1265 1270 1275 1280 1285 1290 1295 1300 1305 1310 1315 1320 1325 1330 1335 1340 1345 1350 1355 1360 1365 1370 1375 1380 1385 1390 1395 1400 1405 1410 1415 1420 1425 1430 1435 1440 1445 1450 1455 1460 1465 1470 1475 1480 1485 1490 1495 1500 1505 1510 1515 1520 1525 1530 1535 1540 1545 1550 1555 1560 1565 1570 1575 1580 1585 1590 1595 1600 1605 1610 1615 1620 1625 1630 1635 1640 1645 1650 1655 1660 1665 1670 1675 1680 1685 1690 1695 1700 1705 1710 1715 1720 1725 1730 1735 1740 1745 1750 1755 1760 1765 1770 1775 1780 1785 1790 1795 1800 1805 1810 1815 1820 1825 1830 1835 1840 1845 1850 1855 1860 1865 1870 1875 1880 1885 1890 1895 1900 1905 1910 1915 1920 1925 1930 1935 1940 1945 1950 1955 1960 1965 1970 1975 1980 1985 1990 1995 2000 2005 2010 2015 2020 2025 2030 2035 2040 2045 2050 2055 2060 2065 2070 2075 2080 2085 2090 2095 2100 2105 2110 2115 2120 2125 2130 2135 2140 2145 2150 2155 2160 2165 2170 2175 2180 2185 2190 2195 2200 2205 2210 2215 2220 2225 2230 2235 2240 2245 2250 2255 2260 2265 2270 2275 2280 2285 2290 2295 2300 2305 2310 2315 2320 2325 2330 2335 2340 2345 2350 2355 2360 2365 2370 2375 2380 2385 2390 2395 2400 2405 2410 2415 2420 2425 2430 2435 2440 2445 2450 2455 2460 2465 2470 2475 2480 2485 2490 2495 2500 2505 2510 2515 2520 2525 2530 2535 2540 2545 2550 2555 2560 2565 2570 2575 2580 2585 2590 2595 2600 2605 2610 2615 2620 2625 2630 2635 2640 2645 2650 2655 2660 2665 2670 2675 2680 2685 2690 2695 2700 2705 2710 2715 2720 2725 2730 2735 2740 2745 2750 2755 2760 2765 2770 2775 2780 2785 2790 2795 2800 2805 2810 2815 2820 2825 2830 2835 2840 2845 2850 2855 2860 2865 2870 2875 2880 2885 2890 2895 2900 2905 2910 2915 2920 2925 2930 2935 2940 2945 2950 2955 2960 2965 2970 2975 2980 2985 2990 2995 3000 3005 3010 3015 3020 3025 3030 3035 3040 3045 3050 3055 3060 3065 3070 3075 3080 3085 3090 3095 3100 3105 3110 3115 3120 3125 3130 3135 3140 3145 3150 3155 3160 3165 3170 3175 3180 3185 3190 3195 3200 3205 3210 3215 3220 3225 3230 3235 3240 3245 3250 3255 3260 3265 3270 3275 3280 3285 3290 3295 3300 3305 3310 3315 3320 3325 3330 3335 3340 3345 3350 3355 3360 3365 3370 3375 3380 3385 3390 3395 3400 3405 3410 3415 3420 3425 3430 3435 3440 3445 3450 3455 3460 3465 3470 3475 3480 3485 3490 3495 3500 3505 3510 3515 3520 3525 3530 3535 3540 3545 3550 3555 3560 3565 3570 3575 3580 3585 3590 3595 3600 3605 3610 3615 3620 3625 3630 3635 3640 3645 3650 3655 3660 3665 3670 3675 3680 3685 3690 3695 3700 3705 3710 3715 3720 3725 3730 3735 3740 3745 3750 3755 3760 3765 3770 3775 3780 3785 3790 3795 3800 3805 3810 3815 3820 3825 3830 3835 3840 3845 3850 3855 3860 3865 3870 3875 3880 3885 3890 3895 3900 3905 3910 3915 3920 3925 3930 3935 3940 3945 3950 3955 3960 3965 3970 3975 3980 3985 3990 3995 4000 4005 4010 4015 4020 4025 4030 4035 4040 4045 4050 4055 4060 4065 4070 4075 4080 4085 4090 4095 4100 4105 4110 4115 4120 4125 4130 4135 4140 4145 4150 4155 4160 4165 4170 4175 4180 4185 4190 4195 4200 4205 4210 4215 4220 4225 4230 4235 4240 4245 4250 4255 4260 4265 4270 4275 4280 4285 4290 4295 4300 4305 4310 4315 4320 4325 4330 4335 4340 4345 4350 4355 4360 4365 4370 4375 4380 4385 4390 4395 4400 4405 4410 4415 4420 4425 4430 4435 4440 4445 4450 4455 4460 4465 4470 4475 4480 4485 4490 4495 4500 4505 4510 4515 4520 4525 4530 4535 4540 4545 4550 4555 4560 4565 4570 4575 4580 4585 4590 4595 4600 4605 4610 4615 4620 4625 4630 4635 4640 4645 4650 4655 4660 4665 4670 4675 4680 4685 4690 4695 4700 4705 4710 4715 4720 4725 4730 4735 4740 4745 4750 4755 4760 4765 4770 4775 4780 4785 4790 4795 4800 4805 4810 4815 4820 4825 4830 4835 4840 4845 4850 4855 4860 4865 4870 4875 4880 4885 4890 4895 4900 4905 4910 4915 4920 4925 4930 4935 4940 4945 4950 4955 4960 4965 4970 4975 4980 4985 4990 4995 5000 5005 5010 5015 5020 5025 5030 5035 5040 5045 5050 5055 5060 5065 5070 5075 5080 5085 5090 5095 5100 5105 5110 5115 5120 5125 5130 5135 5140 5145 5150 5155 5160 5165 5170 5175 5180 5185 5190 5195 5200 5205 5210 5215 5220 5225 5230 5235 5240 5245 5250 5255 5260 5265 5270 5275 5280 5285 5290 5295 5300 5305 5310 5315 5320 5325 5330 5335 5340 5345 5350 5355 5360 5365 5370 5375 5380 5385 5390 5395 5400 5405 5410 5415 5420 5425 5430 5435 5440 5445 5450 5455 5460 5465 5470 5475 5480 5485 5490 5495 5500 5505 5510 5515 5520 5525 5530 5535 5540 5545 5550 5555 5560 5565 5570 5575 5580 5585 5590 5595 5600 5605 5610 5615 5620 5625 5630 5635 5640 5645 5650 5655 5660 5665 5670 5675 5680 5685 5690 5695 5700 5705 5710 5715 5720 5725 5730 5735 5740 5745 5750 5755 5760 5765 5770 5775 5780 5785 5790 5795 5800 5805 5810 5815 5820 5825 5830 5835 5840 5845 5850 5855 5860 5865 5870 5875 5880 5885 5890 5895 5900 5905 5910 5915 5920 5925 5930 5935 5940 5945 5950 5955 5960 5965 5970 5975 5980 5985 5990 5995 6000 6005 6010 6015 6020 6025 6030 6035 6040 6045 6050 6055 6060 6065 6070 6075 6080 6085 6090 6095 6100 6105 6110 6115 6120 6125 6130 6135 6140 6145 6150 6155 6160 6165 6170 6175 6180 6185 6190 6195 6200 6205 6210 6215 6220 6225 6230 6235 6240 6245 6250 6255 6260 6265 6270 6275 6280 6285 6290 6295 6300 6305 6310 6315 6320 6325 6330 6335 6340 6345 6350 6355 6360 6365 6370 6375 6380 6385 6390 6395 6400 6405 6410 6415 6420 6425 6430 6435 6440 6445 6450 6455 6460 6465 6470 6475 6480 6485 6490 6495 6500 6505 6510 6515 6520 6525 6530 6535 6540 6545 6550 6555 6560 6565 6570 6575 6580 6585 6590 6595 6600 6605 6610 6615 6620 6625 6630 6635 6640 6645 6650 6655 6660 6665 6670 6675 6680 6685 6690 6695 6700 6705 6710 6715 6720 6725 6730 6735 6740 6745 6750 6755 6760 6765 6770 6775 6780 6785 6790 6795 6800 6805 6810 6815 6820 6825 6830 6835 6840 6845 6850 6855 6860 6865 6870 6875 6880 6885 6890 6895 6900 6905 6910 6915 6920 6925 6930 6935 6940 6945 6950 6955 6960 6965 6970 6975 6980 6985 6990 6995 7000 7005 7010 7015 7020 7025 7030 7035 7040 7045 7050 7055 7060 7065 7070 7075 7080 7085 7090 7095 7100 7105 7110 7115 7120 7125 7130 7135 7140 7145 7150 7155 7160 7165 7170 7175 7180 7185 7190 7195 7200 7205 7210 7215 7220 7225 7230 7235 7240 7245 7250 7255 7260 7265 7270 7275 7280 7285 7290 7295 7300 7305 7310 7315 7320 7325 7330 7335 7340 7345 7350 7355 7360 7365 7370 7375 7380 7385 7390 7395 7400 7405 7410 7415 7420 7425 7430 7435 7440 7445 7450 7455 7460 7465 7470 7475 7480 7485 7490 7495 7500 7505 7510 7515 7520 7525 7530 7535 7540 7545 7550 7555 7560 7565 7570 7575 7580 7585 7590 7595 7600 7605 7610 7615 7620 7625 7630 7635 7640 7645 7650 7655 7660 7665 7670 7675 7680 7685 7690 7695 7700 7705 7710 7715 7720 7725 7730 7735 7740 7745 7750 7755 7760 7765 7770 7775 7780 7785 7790 7795 7800 7805 7810 7815 7820 7825 7830 7835 7840 7845 7850 7855 7860 7865 7870 7875 7880 7885 7890 7895 7900 7905 7910 7915 7920 7925 7930 7935 7940 7945 7950 7955 7960 7965 7970 7975 7980 7985 7990 7995 8000 8005 8010 8015 8020 8025 8030 8035 8040 8045 8050 8055 8060 8065 8070 8075 8080 8085 8090 8095 8100 8105 8110 8115 8120 8125 8130 8135 8140 8145 8150 8155 8160 8165 8170 8175 8180 8185 8190 8195 8200 8205 8210 8215 8220 8225 8230 8235 8240 8245 8250 8255 8260 8265 8270 8275 8280 8285 8290 8295 8300 8305 8310 8315 8320 8325 8330 8335 8340 8345 8350 8355 8360 8365 8370 8375 8380 8385 8390 8395 8400 8405 8410 8415 8420 8425 8430 8435 8440 8445 8450 8455 8460 8465 8470 8475 8480 8485 8490 8495 8500 8505 8510 8515 8520 8525 8530 8535 8540 8545 8550 8555 8560 8565 8570 8575 8580 8585 8590 8595 8600 8605 8610 8615 8620 8625 8630 8635 8640 8645 8650 8655 8660 8665 8670 8675 8680 8685 8690 8695 8700 8705 8710 8715 8720 8725 8730 8735 8740 8745 8750 8755 8760 8765 8770 8775 8780 8785 8790 8795 8800 8805 8810 8815 8820 8825 8830 8835 8840 8845 8850 8855 8860 8865 8870 8875 8880 8885 8890 8895 8900 8905 8910 8915 8920 8925 8930 8935 8940 8945 8950 8955 8960 8965 8970 8975 8980 8985 8990 8995 9000 9005 9010 9015 9020 9025 9030 9035 9040 9045 9050 9055 9060 9065 9070 9075 9080 9085 9090 9095 9100 9105 9110 9115 9120 9125 9130 9135 9140 9145 9150 9155 9160 9165 9170 9175 9180 9185 9190 9195 9200 9205 9210 9215 9220 9225 9230 9235 9240 9245 9250 9255 9260 9265 9270 9275 9280 9285 9290 9295 9300 9305 9310 9315 9320 9325 9330 9335 9340 9345 9350 9355 9360 9365 9370 9375 9380 9385 9390 9395 9400 9405 9410 9415 9420 9425 9430 9435 9440 9445 9450 9455 9460 9465 9470 9475 9480 9485 9490 9495 9500 9505 9510 9515 9520 9525 9530 9535 9540 9545 9550 9555 9560 9565 9570 9575 9580 9585 9590 9595 9600 9605 9610 9615 9620 9625 9630 9635 9640 9645 9650 9655 9660 9665 9670 9675 9680 9685 9690 9695 9700 9705 9710 9715 9720 9725 9730 9735 9740 9745 9750 9755 9760 9765 9770 9775 9780 9785 9790 9795 9800 9805 9810 9815 9820 9825 9830 9835 9840 9845 9850 9855 9860 9865 9870 9875 9880 9885 9890 9895 9900 9905 9910 9915 9920 9925 9930 9935 9940 9945 9950 9955 9960 9965 9970 9975 9980 9985 9990 9995 9999 10000 10005 10010 10015 10020 10025 10030 10035 10040 10045 10050 10055 10060 10065 10070 10075 10080 10085 10090 10095 10100 10105 10110 10115 10120 10125 10130 10135 10140 10145 10150 10155 10160 10165 10170 10175 10180 10185 10190 10195 10200 10205 10210 10215 10220 10225 10230 10235 10240 10245 10250 10255 10260 10265 10270 10275 10280 10285 10290 10295 10300 10305 10310 10315 10320 10325 10330 10335 10340 10345 10350 10355 10360 10365 10370 10375 10380 10385 10390 10395 10400 10405 10410 10415 10420 10425 10430 10435 10440 10445 10450 10455 10460 10465 10470 10475 10480 10485 10490 10495 10500 10505 10510 10515 10520 10525 10530 10535 10540 10545 10550 10555 10560 10565 10570 10575 10580 10585 10590 10595 10600 10605 10610 10615 10620 10625 10630 10635 10640 10645 10650 10655 10660 10665 10670 10675 10680 10685 10690 10695 10700 10705 10710 10715 10720 10725 10730 10735 10740 10745 10750 10755 10760 10765 10770 10775 10780 10785 10790 10795 10800 10805 10810 10815 10820 10825 10830 10835 10840 10845 10850 10855 10860 10865 10870 10875 10880 10885 10890 10895 10900 10905 10910 10915 10920 10925 10930 10935 10940 10945 10950 10955 10960 10965 10970 10975 10980 10985 10990 10995 10999 11000 11005 11010 11015 11020 11025 11030 11035 11040 11045 11050 11055 11060 11065 11070 11075 11080 11085 11090 11095 11100 11105 11110

Although password access control exists on a host system, which is administered by the host, no mechanism currently exists for a host system to remotely control access to a personal computer.

There are a number of other prior art approaches to PC security. They span the gamut from biometric thumb scan access, to special sealed Tempest shielded PCs to prevent electronic snooping, to DES 5 encryption of all files with specific access passwords on a file or directory level. While such severe measures are certainly warranted in the use and handling of highly sensitive or classified data, this level of security is not generally required or needed in the business environment.

Another threat to the data and programs stored on a PC is attack from a computer virus. These small programs can attach themselves to a normal program or data file, which may be inadvertently copied from 10 system to system. Once a virus program has been copied to a PC, it can cause serious damage to program and data files that reside on the system. Without some form of protection, the PC user may not realize that the system has been infected until after damage has been done.

There are a number of prior art approaches to virus protection. They include never using a disk from anyone, never downloading data from a bulletin board service (BBS) or via a modem, not connecting to a 15 network, checking each program or file with a virus finder, only running new programs on a floppy or on a quarantine machine until determined safe, having a special program slow down the processing of the PC while it watches every activity to determine if is normal or a virus. While these measures can add additional levels of protection, practicality in a business environment must be considered.

Some prior art approaches to virus protection check hard disk system areas and files after the disk 20 operating system has booted. Any damage caused by corrupted system files and data may already be done. If a virus has already attached itself to one of the operating system files, once this file has been loaded (during boot), the virus is in control.

Other approaches to virus protection require booting the system from a known floppy disk and checking the hard disk before allowing the use of files stored on the hard disk.

25 As other approaches to virus protection are resident on disk, they themselves can be corrupted.

Even if you have protected your system from unauthorized access and viruses, once your PC is turned on and validly accessed, it is again vulnerable. Most people turn their PCs on in the morning and leave them on all day. Lunch, an out of the office appointment, long meetings, or just going down the hall are all 30 opportunities for unauthorized access to data. A quick erase or a quick copy to a diskette may leave no signs of activity. However, it is impractical to exit your program, save your data, and turn your PC off every time you leave your desk for a few moments.

A PC screen can also inadvertently expose sensitive data such as payroll, financial, or personnel records to anyone. Information left on the screen while at lunch or a meeting, or obtainable through just a few keystrokes, is all that may be required to steal or destroy a file. In today's aggressive business 35 environment, a company's competitive edge is relative to its customer files and information, or proprietary information such as product development, marketing and sales plans, and product price and costs lists.

Accordingly, it remains highly desirable to provide the ability to detect the presence of viruses in a manner which will allow the operation of the computer to be halted, for example by failing to complete the boot operation, on a regular basis. Furthermore, computer security remains of vital importance.

40 SUMMARY OF THE INVENTION

In accordance with the teachings of this invention, various techniques are employed in order to provide security to a computer system. Certain embodiments are particularly well suited to network environments, 45 and in particular to network environments including one or more PCs. In one embodiment of this invention, tests are performed prior to or during the boot operation in order to determine whether selected programs and/or data files have been corrupted. This may indicate the presence of a virus. In one embodiment, files which will be used during the boot operation are checked for modification prior to allowing those files to be used for system boot. If a potential error is detected, system boot is halted, allowing the user to boot the 50 system from a known, uncorrupted set of files, for example as contained on a floppy diskette. In an alternative embodiment of this invention, additional program and/or data files (which are not used during the boot operation) are checked for corruption either prior to the boot operation or immediately following the boot operation.

In another embodiment of this invention, a unique access diskette is used as a hardware key to allow a 55 user to demonstrate his authorization to gain access to the computer. The unique hardware key is provided by uniquely formatting a standard floppy diskette in such a manner that it contains information indicating the user's authorization to access the system. In one embodiment, this unique formatting is such that the information contained on the access diskette cannot be easily read using the standard diskette reading

technique which is used for reading normal data contained on a normal data diskette, or using the typical software diskette "tool kits" available in the prior art. In accordance with one embodiment of this invention such an access diskette is used in conjunction with user supplied information, such as user I.D., password, and the like, in order to provide two levels of security for the system. If desired, a first level of security can be implemented for users requiring low level access, and a second level of security (including an access diskette) is implemented for users requiring higher level of access, such as system administrators, supervisors, and the like. In accordance with this invention, information contained on the access diskette is provided in a pseudo random fashion, for example, either using a pseudo random number generator or by generating access diskette information in response to information stored in all or parts of the system memory, mass storage device, or the like at the time an access diskette is created. Since information contained in memory, disks, etc., change relatively rapidly, this technique provides pseudo random information for use in creating an access diskette. This information is also stored within the computer for comparison purposes when a prospective user seeks to access the system utilizing a diskette key. In one embodiment of this invention, information stored on the diskette key is also provided by a identification number contained within the computer itself or a portion of the computer hardware dedicated to performing security functions. In this embodiment, the information contained on a diskette key also includes information which, in essence, pertains to the "serial number" of a given computer, thereby preventing this access diskette from being used in another computer for creation of an access diskette for use with that other computer.

In another embodiment of this invention, a method and structure is taught which allows a supervisor or security officer to control security information stored locally in individual PCs remotely, for example via a host computer on the network to which the PC is connected. In this manner, a supervisor or security officer can easily control and update security information pertaining not only to access to the host system, but information which contains user access to an individual stand-alone PC.

In another embodiment of this invention, security from unauthorized access is provided once a valid user has legitimately accessed a computer. In this embodiment, in response to the user pressing a predefined hot key or a predetermined period of time during which the user has not provided input to the computer, selected portions of the computer are disabled, thereby preventing unauthorized access. For example, in response to an elapsed period of time during which the user has not made data or command entry to the computer (for example when the valid user has left the room without logging off) the screen, keyboard, printer, data transmission means, or the like, or various combinations, are disabled, thereby preventing an intruder from observing confidential information during the time the valid user has left the computer. Once disabled, execution of programs currently running or queued to run continues, thereby maintaining computer productivity. Upon entry of appropriate access information by the valid user, the disabled features of the computer are once again enabled allowing full access by the valid user. If desired, this user authorization information to reenable disabled features may comprise a password, a user I.D., a hardware key, such as an access diskette, or the like, or various combinations thereof.

In another embodiment of this invention, access to the computer is made more difficult in response to invalid access attempts. For example, with an increasing number of invalid access attempts, audible and/or visual signals are emanated from the computer with increasing duration, increasing intensity varying pitch, or the like, in order to alert others in the general vicinity that inappropriate activity is occurring on the computer. In one embodiment, once a threshold number of invalid access attempts is reached, the computer is locked up, requiring reboot, thereby increasing the difficulty of a would be intruder to gain access to the computer. In one embodiment, once the threshold value is reached, it is reset to a lower value, thereby requiring the system to be rebooted more frequently in response to a lower number of invalid logon attempts.

These and other features of the present invention will be described by way of the following examples taken in conjunction with the figures.

Figure 1 is a block diagram depicting one embodiment of security hardware constructed in accordance with the teachings of this invention;

Figure 2 is a flow chart depicting a typical PC system boot process which has been modified to include a virus/corrupted file checker in accordance with the teachings of this invention;

Figure 3 is a flow chart depicting in greater detail one embodiment of a virus/corrupted file checker as shown in Figure 2;

Figure 4 is a flow chart depicting one embodiment of an algorithm in accordance with the teachings of this invention which allows security information contained in a local computer to be modified from a remote host computer; and

Figure 5 is a flow chart depicting one embodiment of an algorithm of this invention which provides for

intelligent log on to a computer system.

While certain specific embodiments described herein refer to providing security to PC systems, and PC systems connected in a network, perhaps with a host computer such as a mainframe, it is to be understood that the teachings of this invention are equally applicable to a wide range of computer applications, 5 including computer networks which do not utilize PCs.

Furthermore, a number of specific embodiments are described below. It will be appreciated by those of ordinary skill in the art in light of the teachings of this invention that various combinations of these embodiments may be used in any particular system, or may be provided in a system for selection by a user, thereby providing a large number of permutations of combinations of the various features of this 10 invention.

#### I. Firmware Virus Checker

Figure 1 depicts one embodiment of a security hardware subsystem of this invention which implements 15 an 8KB aged ROM window. This embodiment allows a 16KB EPROM (which contains the virus checker algorithm and, if desired, other various security related firmware) and a 2KB EEPROM (a non-volatile memory device which is used to store security configuration data) to be accessed by the computer from within a single 8KB window. This embodiment minimizes the requirements for system memory space, while also providing an indirect (hidden) access mechanism for the EEPROM device (i.e. protecting secure data).

20 The following description refers to a computer system including a mass storage device, such as a hard disk as found in a typical PC. It is to be understood that the teachings of this invention apply equally well to systems including one or more hard disks, virtual disks, or hard disks partitioned as more than one disk. Furthermore, the teachings of this invention apply equally well to systems utilizing other types of storage media.

25 This invention is particularly well suited for use with desktop or laptop computers which are perhaps more susceptible to viruses than large systems which incorporate sophisticated security schemes. In accordance with the teachings of this invention, a firmware resident program is provided which accesses the file structure of the hard disk before the disk operating system is loaded, in order to verify the integrity of the data and program files on that disk which will be used during the disk operating system boot loading 30 process. In one embodiment of this invention, the system areas checked in a typical IBM compatible PC is shown in Table 1.

TABLE 1

35

#### System CMOS SRAM

Disk Boot Areas (Hard Disk Master Boot Track and  
40 the DOS Boot Sector)

DOS BIO hidden system file (IO.SYS or IBMBIO.COM)

DOS OS hidden system file (MSDOS.SYS or IBMDOS.SYS)

DOS command processor file (COMMAND.COM)

45

AUTOEXEC.BAT

CONFIG.SYS

50

In an alternative embodiment, the method of this invention verifies the integrity of all or a selected set of program and data files in addition to those programs and data files which are used during the disk operating system boot loading process. Since the program of this invention is contained within the computer itself, it 55 eliminates the need to boot from a floppy disk in order to pre-check the hard disk. Furthermore, in one embodiment, the virus checking software is resident in firmware, such as a ROM, and thus occupies no disk space and eliminates the possibility of the virus checking software of this invention itself being corrupted by viruses.

The program of this invention is accessed by the system mother board during adapter board initialization (ROM scan) prior to loading the disk operating system. By residing in the system as firmware, this program is automatically executed upon power up, requiring no operator intervention during its execution. Although in one embodiment the virus checking firmware is executed using the security hardware subsystem shown in Figure 1, any suitable boot ROM hardware architecture could be utilized in accordance with the teachings of this invention. The program of this invention implements algorithms necessary to read selected data and program files from the system hard disk, without requiring the services of the disk operating system.

5 Prior to running the virus checking program of this invention for the first time, the critical system data and program files (such as are required for system boot), as well as any other files previously specified by the user, are scanned and a proprietary signature (e.g. a CRC signature) is created for each file. These signatures are stored in non-volatile memory for later use during virus checking prior to system boot. As additional files are created or added to the hard disk and designated by the user as files which are to be virus checked prior to subsequent boot operations, additional signatures are created for each, and stored in 10 the non-volatile memory for use during virus checking prior to subsequent system boots.

15 In one embodiment of this invention, a 32 bit CRC algorithm is used which in fact comprises a combination of two different 16 bit CRC algorithms. In this manner, the likelihood of a virus modifying a file and avoiding detection is significantly reduced as compared to the embodiment where a single CRC algorithm is used. Thus, for example, while a sophisticated virus may intentionally or by chance modify a 20 file in such a way that the CRC for the file remains the same, such a virus will most likely not provide unchanged CRC signatures for more than one CRC algorithm.

25 Figure 2 is a flow chart depicting a typical PC system boot process which has been modified to include the virus checking algorithm of this invention. As shown in Figure 2, upon power up, BIOS motherboard diagnostics are performed, in a well known manner. Following this, the BIOS system RAM test is performed and the BIOS hardware initialization step performed. Then the BIOS ROM scan takes place. All of these steps are well known in the prior art and can be performed in any desired fashion. Of interest, at any desired point during BIOS ROM scan, the firmware virus/corrupted file checking algorithm of this invention is performed, and if any potential problems are detected, a warning is given to the user and system boot is 30 halted in order to allow the user to take appropriate action. Such appropriate action in the event of the detection of a potential problem might be booting the system from a floppy diskette which is known to be free of viruses. As shown in Figure 2, following successful completion of the firmware virus check in accordance with the teachings of this invention, BIOS ROM scan continues following which the system is booted from the hard disk in the normal manner.

35 Referring to Figure 3, a more detailed explanation of the operation of one embodiment of the firmware virus/corrupted file checker of this invention is described.

1. The table of previously created CRC signature is retrieved from non-volatile memory.
2. The system CMOS area is scanned and a CRC is calculated. The new CRC is compared with the old CRC and differences are posted for example, to a data log, the screen, or a printer. Any errors at this point abort further testing.
3. Since DOS has not been booted, DOS has not yet created tables of information regarding, for example, file pointers describing locations of system files on the hard disk. Thus, the virus/corrupted file checker of this invention reads the disk boot areas from disk into a buffer. Disk structure information is extracted from the boot information and from various system BIOS services, and a disk information table is built in the computers RAM in order to allow the virus/corrupted file checker of this invention to access, for example, system files contained on the disk.
4. A CRC is calculated for the disk boot information currently in the buffer. The new CRC is compared with the old CRC and differences are posted. Any errors detected at this point aborts further testing.
5. The root directory of the disk is scanned and a look-up-table is built which contains starting file allocation table (FAT) offsets and sizes for the remaining system files to be checked.
6. The BIO system file is read into a contiguous buffer and a CRC is calculated. The new CRC is compared with the old CRC and differences are posted.
7. The DOS system file is read into a contiguous buffer and a CRC is calculated. The new CRC is compared with the old CRC and differences are posted.
8. The COMMAND system file is read into a contiguous buffer and a CRC is calculated. The new CRC is compared with the old CRC and differences are posted.
9. The AUTOEXEC file is read into a contiguous buffer and a CRC is calculated. The new CRC is

compared with the old CRC and differences are posted.

10. The CONFIG file is read into a contiguous buffer and a CRC is calculated. The new CRC is compared with the old CRC and differences are posted.
11. If any errors are detected, system boot is halted in order to allow the user the opportunity to boot from a recovery diskette or alternate DOS diskette, if desired.

5 Once the algorithm of this invention has been executed, control is returned to the system BIOS to allow continuation to the normal DOS boot process, as shown in Fig. 2.

When the program of this invention is executed prior to disk operating system boot, each of the system data areas and files are scanned, and signatures calculated. These new signatures are then compared with 10 the values stored in non-volatile memory. Any differences are reported as an integrity failure with specific data or program files. If a failure is detected, the user is given the option to boot from a recovery diskette, thereby allowing the system to be booted from a disk containing a disk operating system known to be 15 uninfected by a virus. Thus, the computer becomes usable and the user is able to investigate the potential problems on the hard disk, and allows the replacement of potentially infected or corrupted program and data files. By restoring corrupted files prior to their use during boot or subsequent execution of applications software, possible system disaster can be averted by preventing the spread of a virus throughout the system.

10 This teachings of this invention are suitable for use in any type of device which loads critical operating system information from hard or soft disk media, where potential contamination by a virus could have 20 dangerous impact, for example: process control, power plants, launch control, lottery, communications center, data routing systems, electronic funds transfer, and the like.

In one embodiment, specific program or data files which have been previously specified by a user are automatically checked after the system has booted. If any of the selected files have been modified, indicating a potential problem, including the presence of a virus, the user will be notified of the change.

25

## II. Access Diskette

In accordance with the teachings of this invention, a diskette is uniquely formatted using a method which is non-standard for the resident disk operating system. This diskette is then capable of being read 30 and verified by resident security software so that it may be used as a hardware key to access the system. Of importance, in accordance with teachings of this invention, a diskette key is provided which utilizes standard floppy disks, rather than special hardware or key devices as known in the prior art. However, the standard floppy disk which is formatted according to the teachings of this invention in order to serve as an 35 access key cannot be read or copied by standard operating systems utilities or after-market disk utility programs.

In one embodiment of this invention, the algorithm used to create access diskettes is based on two randomly generated signatures (numeric values) such that all access diskettes (with the exception of a backup access diskette, if desired) are unique in two ways:

1. Each access diskette is uniquely formatted; and
2. Each access diskette contains different "key" information.

40 In one embodiment, the signature values which are used to create access diskettes are generated such that they are unique for a given PC, and unique from one creation time to another. If desired, a mechanism is also provided to manually supply the signature values during access diskette creation.

The access diskette is read and verified by resident software (or firmware) which requires a valid 45 access diskette before access to the system is allowed. The access diskette may be used as a "stand-alone" key to the system or may be used in conjunction with a password to "double-lock" the system.

In accordance with one embodiment of this invention, a password is used in conjunction with the access diskette in order to control access to the computer. In an alternative embodiment of this invention, certain 50 passwords (e.g. a User password) are sufficient to obtain access the computer without the use of the hardware access diskette. The access diskette must be used, however, to obtain a higher level of access, for example that level which is available when utilizing a Supervisor password.

An access diskette of one embodiment of this invention comprises three parts:

- (1) Identification information indicating this is an access diskette. This identification information is stored in a portion of the diskette which will be referred to as the identification sector or identification track.
- 55 (2) An access signature, which is preferably unique for a given system. The access signature is stored in a portion of the access diskette called the key sector or key track.
- (3) The remainder of the diskette.

The identification information indicating this is an access diskette need not be used for the purpose of

controlling access to a specific PC and thus can be the same for each system. In one embodiment, a copyright notice is conveniently used for this purpose.

The access signature is comprised of two portions, a value specifying the location on the access diskette where the signature is located, and a signature which is uniquely assigned to a given access diskette.

In one embodiment, the location on the access diskette where the access signature is located is defined by a 32-bit key value which is mapped as shown in Table 2. Naturally, it will be readily appreciated in light of the teachings of this invention that any desired number of bits can be used to specify the location of the access signature on the access diskette, and a number of arrangements for bit mapping of this information is possible within the spirit of this invention.

TABLE 2

HIGH WORD			LOW WORD		
not used	5 bit track pos.	8 bit sector offset	H E A D	7 bit track #	8 bit Sector #
bits	bits	bits	bit	bits	bits
31-29	28-24	23-16	15	14-08	07-00

The key track contains the sector ID number specified in the location key in the position (i.e., the 4-bit track position field) specified by the location key.

For example, if the specified sector ID is 123 and the position code is 4, each formatted track contains the sector ID in the order shown in Table 3.

TABLE 3

Track Pos	0	1	2	3	4	5	6	7	8
-----									
Sector ID	119	120	121	122	123	124	125	126	127

After the key track is formatted, the signature is written to the key sector (sector ID 123 in the example of Table 3) at the offset specified in the location key value (i.e. the 8-bit sector offset field). The key sector can also contain a usage count immediately following the signature bytes, as well as any other desired data.

Then, the first sector ID (sector 119 in the example of Table 2) is reformatted as the sector number containing information indicating that this is an access diskette.

The identification sector is then prepared and written to the diskette in the reformatted sector. In one embodiment, the identification sector includes the 32-bit key value. In one embodiment, the key value is derived from the board identification number (BIN) of the security hardware of this invention, in order to prevent a single access diskette from being valid in more than one PC. Without a unique signature in the identification sector, it is possible for a single diskette to be used to create a valid access diskette in more than one PC, because the key track/sector/head varies from one system to the next.

The verification process reads the two significant sectors (the key sector and the identification sector) and ensures that the system specific information and the identification information are valid. If an error occurs reading the access diskette during verification, it is assumed to indicate an invalid access diskette and access is refused.

In one embodiment of this invention, the access signature is a 32-bit value which is unique to a particular access diskette. If desired, however, a duplicate access diskette is created at the same time an

access diskette is created.

In one embodiment, the access signature is created as the current (at the time the access diskette is created) CRC of a portion of the system data. For example, a CRC of the file allocation table (FAT) may be created, or of a specified portion of the hard disk, or the RAM, or a specified portion thereof. Alternatively, 5 additional hardware memory (such as the non-volatile memory used for storing security information, such as is described above with regard to virus checking) is used to create the access signature. Using the current CRC as a location code insures that the creation of each key disk is unique. A lookup table is provided such that each authorized key disk value is stored and checked upon insertion of a key disk for login purposes. A system administrator is able to delete undesired previous key disk access signatures as they become no 10 longer required.

In one embodiment, the remainder of the access diskette, i.e., that portion of the access diskette which is not used to store the identification information notice or the access signature, is ignored, leaving a large number of unused tracks. In an alternative embodiment, the remainder of the access diskette is filled. In this embodiment, the unused tracks are preferably filled such that the diskette contains a large number of 15 unused tracks which are filled with data which appear substantially similar to the data stored in the tracks used to store the identification information notice and access signature. For example, each unused sector is written to store a pattern similar to that stored in the key sector which stores the access signature except, of course, that the access signature is not contained within the key sector. This makes it very difficult for an unauthorized person to read the access diskette and determine the access signature.

20 III. Local Information Modified or Controlled by Remote Host

In accordance with one embodiment of this invention, a unique process is provided by which a remote host computer system may access a local desktop or personal computer and modify its information. This 25 information may be data, whereby the host computer can modify local computer data, for example as the master information stored in the host changes, or in order to encrypt or decrypt information which is stored in the local computer. Alternatively, or in addition thereto, this information which is capable of being modified or controlled by the remote host computer can be local security information, thereby allowing the host to remotely control access to the PC. This allows system administrators to control access to individual 30 PCs remotely, via the host computer system. The teachings of this invention may be used to remotely change information stored in the PC which determines whether a user may gain access to that PC, such as authorized user ID and password information. It is also possible for the host to update information stored within the PC which serves as a table of information which is authorized to be accessed by one or more users. System administrators may also use the remote system of this Invention to remotely access use 35 information stored within the PC, such as date and time information associated with each successful and/or unsuccessful attempt to log into the PC.

Figure 4 is a flow chart depicting one embodiment of this invention for use in a network including a host computer and a PC having local security information which is capable of being modified from the remote host. As shown in the flow chart of Figure 4, a first step in this embodiment is that the PC logs into the host 40 system, for example in any one of a number of well known ways, following which the PC is connected to the host computer as shown in Step 2. In Step 3, the host modifies or updates selected information in the PC, such as the user ID and/or password information of valid users. In Step 4, the host checks the audit log of the individual user of the PC system in order to determine user audit log information. In the event that the audit log indicates unauthorized activities, the host computer causes user access to be revoked.

45 Conversely, if the check of the audit log of the individual PC user determines no reason to forbid access to the host computer, operation branches to box 5 in which the host computer requests and receives from the PC a password from the PC user. In Step 6, the host computer modifies a list of allowable data files which may be accessed by one or more users. Secure data associated with the user, as shown in Step 7, is downloaded from the host to the PC. This secure information is appropriately stored within the PC for later 50 use by the PC.

In one embodiment, as shown in Step 8, this secure data is not stored on the disk of the PC where it might be undesirably retrieved by a potential intruder. This allows greater control of secure information since the data stored in memory is erased when the PC is turned off. In this embodiment (for example as shown in Fig. 1), such security information is stored in hardware contained within the PC, for example in 55 nonvolatile memory (such as an EEPROM) located in an area of the PC dedicated to security functions, such as a security card installed in one of the expansion slots.

As shown in Step 9, the host computer then allows the PC to be used as a work station with access to the host computer.

IV. Active System Security

In accordance with one embodiment of this invention, a unique system is taught which allows an active computer system to be secured from use without disabling the processing capability of the system.

5 In this embodiment, computer applications are protected from unauthorized use via screen blanking and/or keyboard lock with password unlock. In one embodiment, the user may blank the screen at will via a previously defined hot key, and/or the screen will blank automatically after a user-specified period of inactivity (automatic timeout). In addition to screen blanking, the keyboard is locked and disabled from normal use until the proper password is entered via the keyboard. This password may or may not be the  
 10 same as the password required for initial logon to the system. This automatically protects the PC from access while the user is away for a specified period of time.

Although the screen is blanked and the keyboard locked from normal use, any processing which is currently underway on the PC continues, thereby maintaining productivity. In addition to the opportunity to cause screen blanking and keyboard lock, other computer functions can be disabled as well, as desired. For  
 15 example, if a lengthy and confidential report is printing or will be printed following lengthy processing, it may be desirable to disable printing when the user leaves the room, as indicated by his pressing a predefined hot key his or failing to make keyboard entry for a predetermined period of time. Other input/output functions such as data communication (either transmission, reception, or both) can be disabled in a similar manner.

20 In an alternative embodiment, upon an appropriate timeout or in response to the user pressing a previously defined hot key, the screen is blanked and a prompt for entry of the user password is provided on the screen. In this embodiment, the data contained on the screen disappears so as not to be visible to unintended eyes, yet a prompt appears indicating to the user that all is well with the computer and that upon entry of a correct password, the user will regain access.  
 25 In another embodiment, attempts to gain access once the screen has blanked are recorded, alternatively, only unsuccessful attempts to access are recorded. Information pertaining to these attempts, such as the time at which they occur, or their number, or even the unsuccessful passwords, are made available to the authorized user when he regains access to the system by entering the correct password.

30 V. Intelligent Access Control

In accordance with one embodiment of this invention, an access control program or software package dynamically alters its defense tactics, making it progressively more difficult to illegally access the system. For example, if it is determined that excessive attempts are being made to enter a password, a series of  
 35 tones are sounded to alert others in the vicinity, thus discouraging anyone illegally trying to access the system by trial and error.

In one embodiment of this invention, all logon accesses to the system are tracked by maintaining an access log or audit trail. The access log indicates the date and time of both valid logons and invalid logon attempts. The user may configure the system such that, after each valid logon, the access log table and/or  
 40 a message is provided (such as a written message or a beep tone) indicating if any invalid attempts have been made to logon to the system.

Figure 5 is a flow chart depicting the operation of one embodiment of a system constructed in accordance with the teachings of this invention. Box 1 is the starting point, or entry into this embodiment of a routine operating in accordance with the teachings of this invention. This occurs, for example, upon power  
 45 up of the computer, upon reboot, or when access to the computer is desired by a user. Not shown in this flow chart is the step of configuring the threshold level. This occurs only once a user having valid authority has successfully logged onto the system and entered a configuration step, whereby one or more threshold values are set and stored for use during future logon attempts.

Box 2 requests and accepts from the user login information, such as user I.D. and password. Decision  
 50 Step 3 determines whether the login attempt is valid, i.e. whether the login information is correct according to authorized login information stored in the computer. If the correct login information is received, control passes to Step 4 which, if desired, displays valid and/or invalid login information. For example, this step indicates to the authorized user who has just gained access, the number of, or specific information related to, authorized and/or unauthorized login attempts. If desired, this information can be limited to login  
 55 attempts which occurred since this user's last authorized login, or from a specified date or time. Alternatively, various techniques can be used to otherwise limit the amount of login information displayed, for example when a specified number of failed login attempts occur within a given short period of time, which is indicative of an unauthorized user attempting to gain access to the system by trial and error. This

login audit log information is, in one embodiment, also available for remote polling by a host system, thereby allowing a system administrator to become alerted to attempted breaches of security at the PC level.

Conversely, if in Step 3 an invalid login attempt is detected, control passes to decision Step 5 which 5 determines if this is the first invalid login attempt during a specified period of time, for example since the last valid login, or during a particular time period. If it is determined that this is the fist invalid login attempt according to the criteria used by decision Step 5, control passes to Step 6 and the computer beeps twice as an indication of an invalid login attempt. This audible signal is not too distracting but may alert others in the area to pay particular attention if additional error signals are heard. Control is then passed to block 2, 10 allowing the user to attempt to login again. Conversely, if Step 5 determines that an invalid login attempt was not the first, control is passed to decision Step 7 where it is determined if the invalid login attempt was the second invalid login attempt. If so, control passes to Step 8, wherein the computer beeps several times prior to passing control back to Block 2. This will allow others in the vicinity to notice that something is awry and perhaps call security or take their own steps in order to determine the identity of this would-be intruder.

15 Conversely, if decision Step 7 determines that the invalid login attempt was not the second invalid login attempt, control is passed to block 9 which initiates action commensurate with the fact that three or more invalid login attempts have been detected. Control is passed to block 10 wherein the computer system is locked, for example by halting the system microprocessor, requiring the system to be rebooted (either hot or cold, as specified by information to which block 10 responds which information has been previously 20 supplied by a legitimate user). This requires that the computer be rebooted, as shown in Step 11, prior to returning control to Step 2, which again allows a user to attempt to obtain access. Upon reboot, the threshold is set to one, thereby allowing only one password access failure before locking up the system and thereby requiring a reboot. Thus, after the initial threshold value (in this example, 3) of unsuccessful login attempts is reached, the system is locked up and must be rebooted, after which only one invalid login 25 attempt is allowed before requiring the system to be rebooted. In one embodiment of this invention, the programmable threshold value is reset to its normal value (in this embodiment, 3) in response to to a valid login.

By requiring the system to be rebooted after a predetermined number of failed login attempts, considerable difficulty is encountered by the unauthorized user who is attempting to illegally gain access to 30 the system. For example, rather than being able to rapidly enter a large number of potentially correct passwords on a hit or miss basis, the process is considerably slowed by the need to reboot the computer after three failed login attempts. In addition, audible signals from the computer indicating failed attempts will alert others in the physical proximity of the computer that something inappropriate is happening.

Naturally, other embodiments of this invention will become readily apparent to those of ordinary skill in 35 the art in light of the teachings of this invention, for example, additional decision steps such as steps 5 and 7 may be employed so that any number of security threshold levels may be provided. For example, in one alternative embodiment, no audible signal is provided in response to a first invalid login attempt, as often occurs due to a simple typographical error by a user during his login attempt. In response to a second invalid attempt, the computer beeps twice; in response to third, fourth, and fifth invalid attempts, the 40 computer beeps five times; and in response to the sixth invalid attempt the computer locks up, requiring reboot. This as well as numerous other variations are all within the scope of this invention.

Other alternative embodiments include not merely increasing the number of audible tones in response to an increasing number of failed logon attempts, but varying their intensity, pitch, or the like. For example, in response to an additional one or two failed logon attempts, a simple beep may be sounded while in 45 response to a third failed logon attempt, a lengthy and loud wailing sound might be produced. Furthermore, in addition to audible signals, unique visual patterns may be flashed upon the screen, perhaps frightening the intruder away, and possibly alerting others in the area that something inappropriate is occurring on the computer.

## 50 VI . Non-Volatile Security Configuration Data Storage

A mechanism is provided for the storage of security configuration and audit data in a non-volatile storage device, such that the data can be error checked and corrected and protected from tampering.

In this embodiment, security data is stored in non-volatile memory (e.g. hardware incorporated in the 55 security hardware shown in Figure 1) which eliminates the need to store on an easily accessible hard disk.

In this embodiment, data is structured in redundant tables whose contents are monitored via both checksum and CRC algorithms. By containing embedded checksums and CRC, the data can be readily checked for corruption. The redundant table structure provides a mechanism for automatic data recovery

(correction) should one of the tables become corrupted.

Error checking and correction are provided through firmware access routines. The checking and correction processes are transparent to the application.

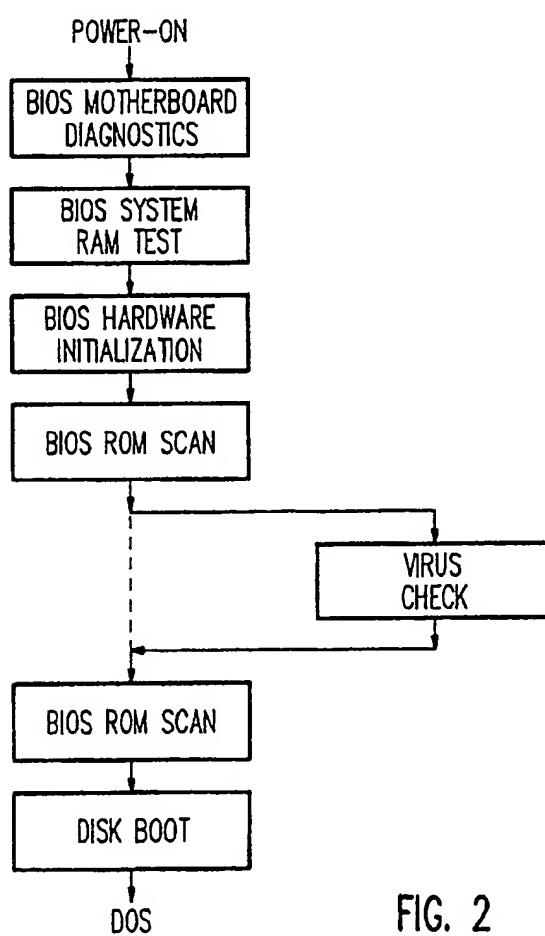
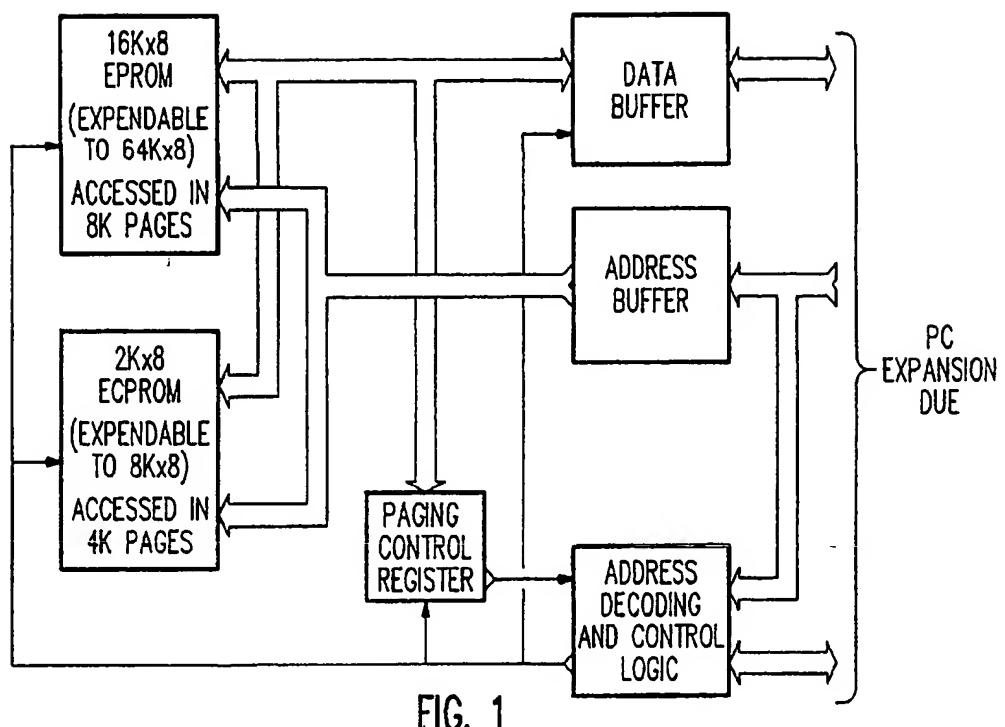
The invention now being fully described, it will be apparent to one of ordinary skill in the art that many changes and modifications can be made thereto without departing from the spirit or scope of the appended claims.

### Claims

10. 1. A method for detection of computer viruses or corrupted files, comprising the steps of:  
 initiating a system boot;  
 calculating signature values for one or more files stored in said computer storage;  
 comparing said signature values with previously calculated and stored signature values for said one or more files; and  
 15 halting system boot if said step of comparing determines that one or more of said calculated signature values differs from its corresponding one of said previously calculated and stored signature value.
2. A method as in claim 1 wherein said one or more files comprise files which will be used during the boot operation of said computer.
20. 3. A method as in claim 2 wherein said one or more files further comprise user specified files which may or may not be used during the boot operation of said computer.
25. 4. A method as in claim 1 wherein each of said signature values are calculated using more than one method.
30. 5. A method as in claim 4 wherein each said signature value comprises a plurality of sets of bits, each said set of bits calculated in accordance with an associated signature method.
35. 6. A method as in claim 1 wherein said previously calculated and stored signatures are stored in a memory area other than computer memory used for normal operation of the computer.
7. A method as in claim 6 wherein said memory area other than said computer memory can not be accessed by normal operation of said computer after system boot.
35. 8. A method as in claim 1 wherein said step of initiating a system boot comprises the step of initiating a system boot from secure firmware.
40. 9. A computer system comprising:  
 mass storage means;  
 boot files, stored in said mass storage means, which are used during a system boot operation;  
 means for storing signature values associated with said boot files;  
 means for generating a system boot signal;  
 45 means for calculating signature values for said boot files in response to said system boot signal;  
 means for comparing said calculated signature values with corresponding values which have been previously calculated and stored in said means for storing signature values; and  
 means for preventing system boot if one or more of said calculated signature values differs from its corresponding value which has been previously calculated and stored in said means for storing signature values.
50. 10. A method for securing access to a computer system comprising the steps of:  
 preventing access to said computer system until access authorization is verified;  
 receiving an access diskette in a standard diskette drive normally used for data transfer between said computer system and storage diskettes;  
 55 causing said standard diskette drive to read at least a portion of the contents of said access diskette using a technique different from the technique used by said standard diskette drive to read data from storage diskettes; and

allowing access if said access diskette contains valid authorization information.

11. A method for storing security information in a computer network comprising a plurality of computers, comprising the steps of:
  - 5 causing a first one of said computers to transmit data for storage in a second of said computers, said information serving to control user access to said second computer.
12. A method for controlling a computer comprising the steps of:
  - 10 during operation of the computer, detecting the occurrence of either:
    - entry of a selected command from a user; or
    - an elapse of a selected amount of time during which there has been no data or commands inputted by the user;
    - 15 in response to said occurrence, performing the following steps:
      - disabling one or more input/output functions of said computer;
      - monitoring for user input of information indicating valid user authorization for use of said computer; and
      - in response to the detection of valid user authorization, enabling said one or more input/output functions of said computer which had previously been disabled.
  - 20 13. A method as in claim 12 wherein said one or more input/output functions are selected from the group of functions consisting of keyboard entry, data entry, screen display, printer output, and data transmission.
  - 25 14. A method as in claim 12 wherein selected functions of said computer are not disabled in response to said occurrence.
  15. A method as in claim 14 wherein said selected functions comprise computer processing.
  - 30 16. A method as in claim 14 wherein said selected functions comprise execution of programs currently being run, or in a queue to run, at the time said occurrence is detected.
  17. A method as in claim 12 wherein said information indicating valid user authorization comprises a hardware access key, user identification, password information, or a combination thereof.
  - 35 18. A method for controlling access to a computer comprising the steps of:
    - receiving user authorization information from a prospective user;
    - determining if said user authorization information is valid;
    - if said user authorization information is valid, allowing said prospective user to have access to said computer; and
    - 40 if said user authorization information is invalid, increasing the difficulty of gaining access to said computer.
  19. A method as in claim 18 wherein said step of increasing the difficulty of gaining access to said computer comprises the steps of increasing the amount or intensity of error signals provided in response to invalid user authorization information.
  - 45 20. A method as in claim 18 wherein said step of increasing the difficulty of gaining access to said computer comprises the step of requiring said computer to be rebooted in response to a number of invalid user authorization attempts exceeding a threshold number of invalid user authorization attempts.
  - 50 21. A method as in claim 20 wherein said threshold number is reduced to a lower threshold number following a number of invalid user authorization attempts which equals or exceeds said threshold number.



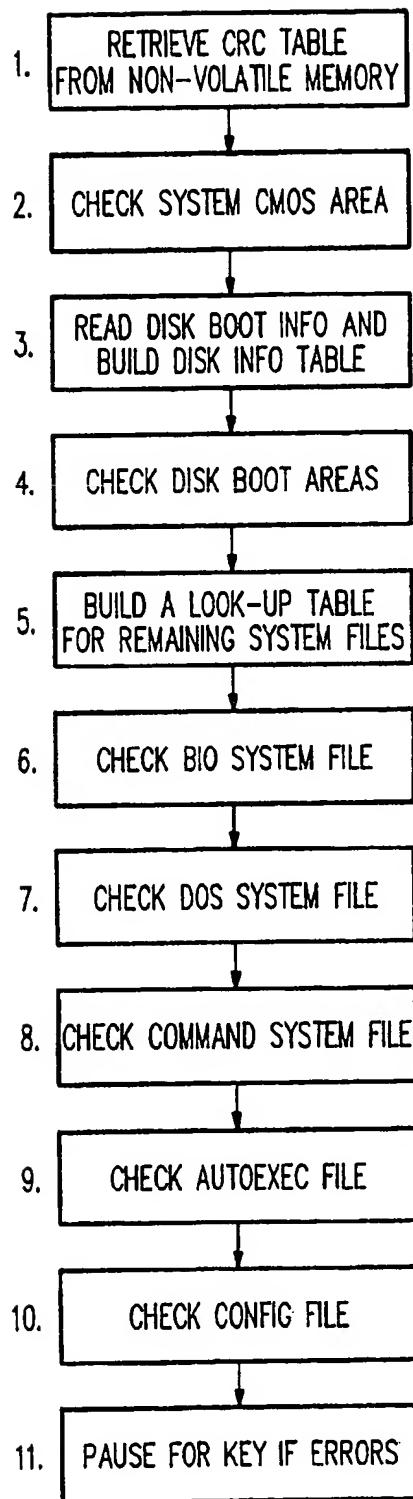


FIG. 3

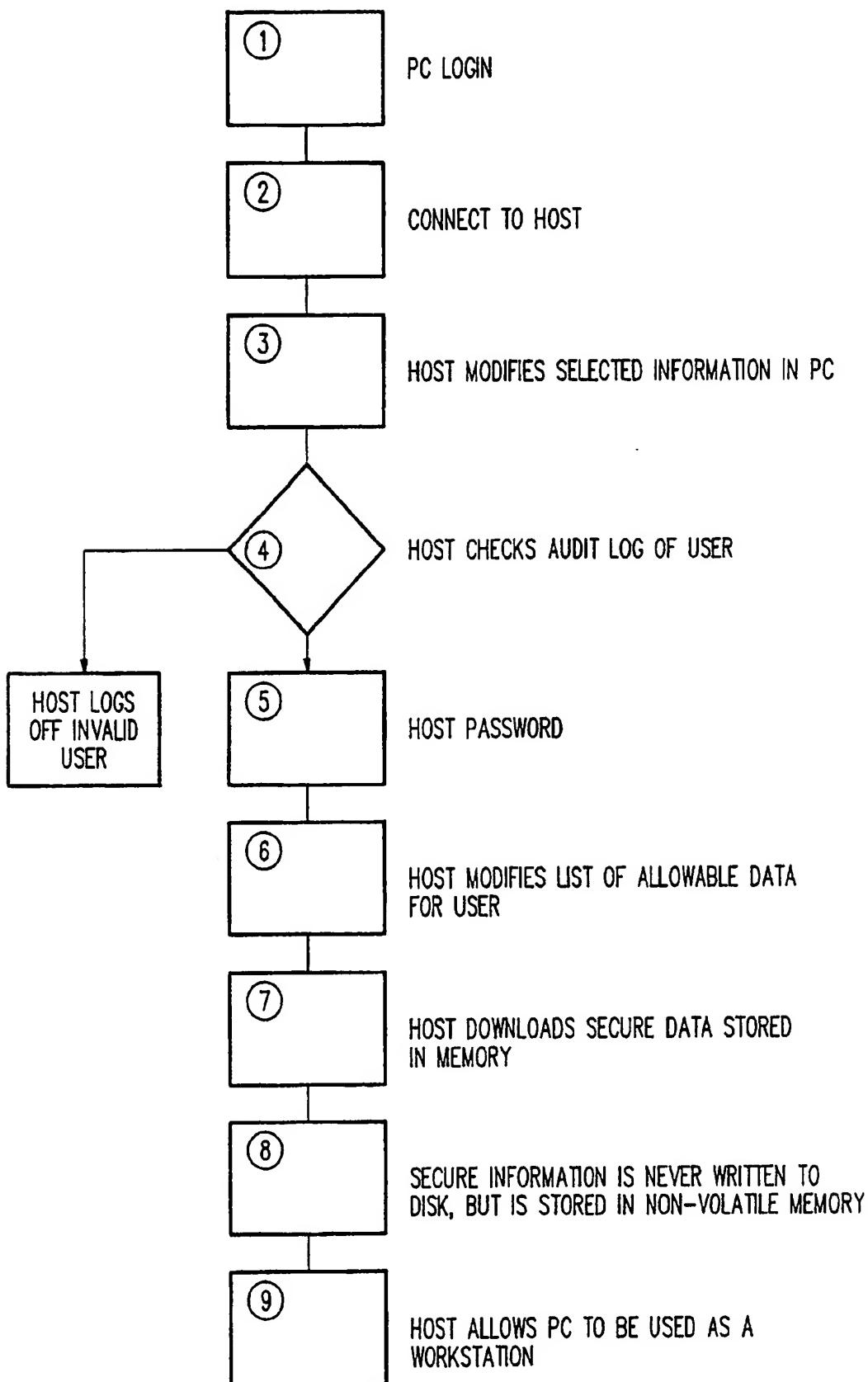


FIG. 4

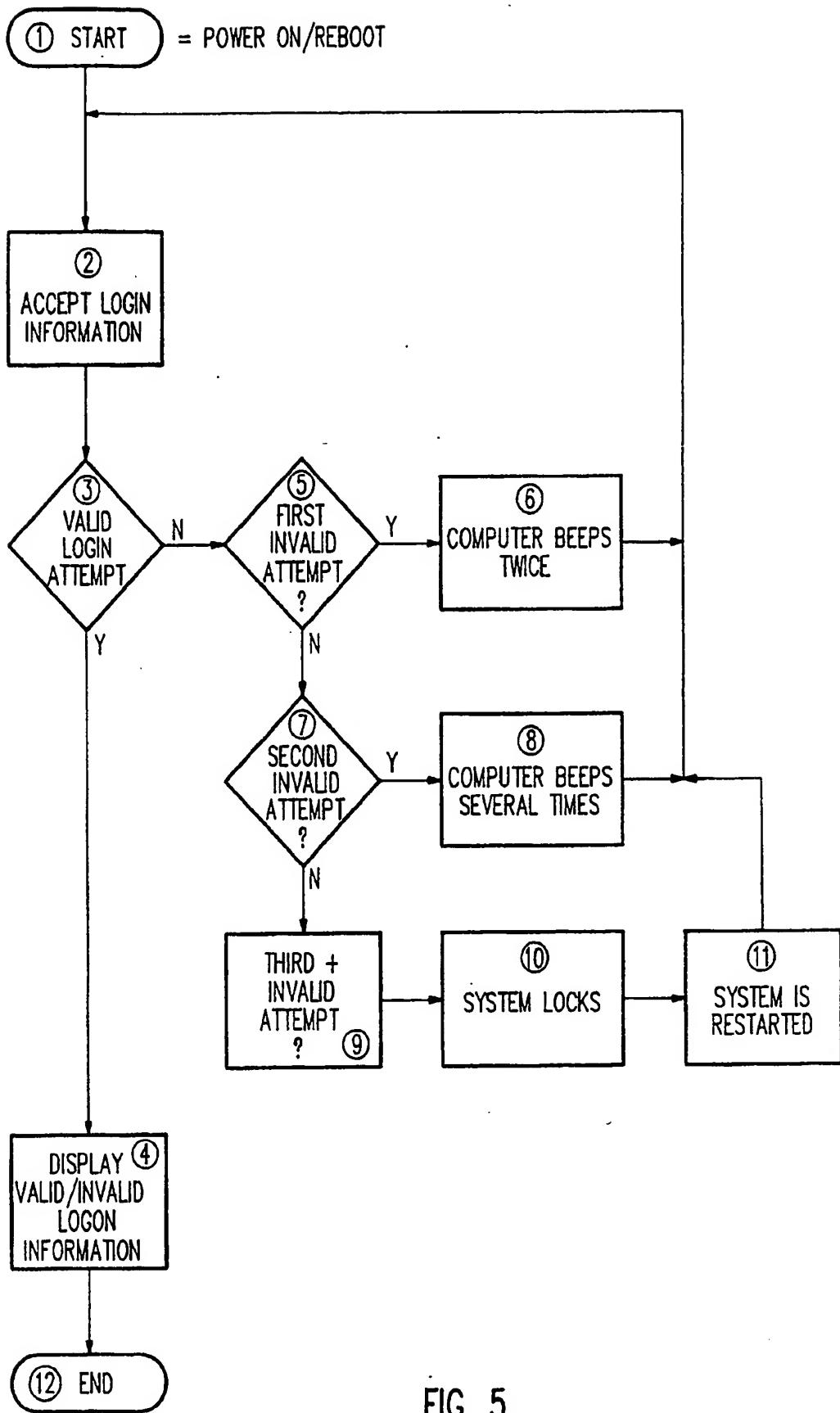


FIG. 5